DEPARTMENT OF HOMELAND SECURITY

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

FULL COMMITTEE MEETING

WEDNESDAY, March 21, 2007

Crowne Plaza Washington National Airport

Arlington Ballroom

1480 Crystal Drive

Arlington, VA 22202

AFTERNOON SESSION

MR. BEALES: Our first panel this afternoon is to talk about IT transformations within the U.S. Citizenship and Immigration Services. With us is Daniel Renaud who's the Chief of the Transformation Program Office. I can think of many agencies that could use a transformation program office. He became the chief in January of 2007 and had been serving as the Acting Chief of the TPO since December of 2005. Mr. Renaud is responsible for overseeing the agency's transition from a fragmented and paper-based filing system to a centralized and consolidated electronic adjudication system. He manages development of strategies, government and contractor resources and the funding and recommends courses of action for the transformation leadership teams. Prior to this position he served as the Director of the Performance Management Division. Also with us today is Gerri Ratliff who's the Chief of the Verification Division of CIS. That division, the Verification Division oversees the basic pilot employment eligibility verification program and the SAVE agency benefit program. Since joining the federal government in 1990 Gerri has held numerous positions with USCIS, the former Immigration and Naturalization Service and also in the Justice Department and the Office of Management and Budget handling a range of immigration-related policy and legislative issues. She has a BA in Journalism and Speech Communication from University of North Carolina, a JD from Washington College of Law at American

University and a Masters in Public Administration from the Kennedy School at Harvard. Mr. Renaud?

MR. RENAUD: Thank you very much. As you indicated, I'd like to speak today and give you an update on the USCIS transformation effort, what we're doing, why, what our plans are to transform our agency from a paper-based processing group to a more electronic, more streamlined user- friendly entity.

First of all, USCIS processes immigrant and non-immigrant based benefits as well as requests for naturalization to become citizens of the United States. Just to give you an idea of what that means for those who may not know, our workloads are divided into several lines of business including family-based immigration, employment-based immigration, asylum and refugee line of business, naturalization, special status programs such as temporary worker - such as, sorry, temporary protected status and document issuance to validate that someone is in fact - holds a particular status in the United States and that includes document production, document renewal. Along all of these lines of business we have several key themes, not the least of which is national security and in all of our lines of business we have a national security role that we play. We support the efforts of DHS department-wide as well as other government agencies, law enforcement agencies, et cetera. Also Gerri Ratliff will be speaking about another key component of USCIS business which is employment eligibility verification. USCIS has realized for awhile that it needs to change the way it does business. It needs to break out of a legacy model that has really hampered our ability to improve service, to streamline benefits processing and to better enable the agency to identify those high-risk applicants, to distinguish those from the low-risk applicants and treat both appropriately. Currently there exists significant gaps in our business process and in the supporting technologies that impair our ability to achieve our objectives of national security, customer service and operational efficiency. Legacy processes and supporting technologies were not designed for and are not capable of meeting the needs of the 21st century and an immigration environment in that. Currently it's difficult for USCIS to align our resources with our workload which was a major contributor to our building a backlog of benefit applications over the past few years which we've spent the last few years eliminating. But essentially we have a system that relies on either moving paper to available resources, or moving available resources to the paper applications, neither of which is efficient or cost-effective. We do not have the capability to verify the identity of applicants and manage that identity throughout the process.

We need to do a better job department-wide of making sure that we know who we're dealing with, and again this both streamlines the process for those people who say they are who they are as well as identify those people who don't and can help us take appropriate action there. We need to do a better job of sharing information with our DHS

partners. As you can imagine, in a paper environment, and you'll be hearing from some of our Office of Record Services later on this afternoon, we have about - they'll correct me, but somewhere around 100 million A files and receipt files, 100 million paper files that we manage on a daily basis. Of the data in those files, a very small amount of it is electronically captured and able to be able to be shared in a timely and effective and complete manner. We need to do a better job of that. We are, as you can imagine, 100 million files is quite a bit of information that is used to support the department mission. And we need to do a better job to share that more timely, more completely, more accurately.

And as we have a legacy IT environment of systems that were designed around form types, around benefit types, what has resulted is a system where legacy systems don't really speak to each other very well so we ask people when they file for applications to submit the same application again and again and again. And I know I saw some of the companies and attorney firms represented here by the board and I'm sure you know what I'm talking about provided you do immigration business. I don't know how many annual reports that we have in our A files, but we essentially ask for the same documents again and again and again, and that's just not smart for anybody.

USCIS has taken a - we've spent several years trying to transform our business and we've had several initiatives over the past years that have been successful to a certain degree, none of which fully realized their vision. I think we've taken prudent steps this time to get it right. We've elevated the Transformation Program Office from out of an individual directorate domestic operations to report directly to the deputy director. So we have a single authoritative decision point that will help guide decisions and strategies across the agency. We believe that with the organizational placement we'll be much more effective and much more able to meet our goals.

As I said, we will be transforming from a paper-based process to an electronic end-to-end process. We will increase our ability to share data with immigration partners. We'll improve security by being able to uniquely identify individuals, to create customer accounts in much the same way that online businesses do so people have, if you want to think of it as a personal webpage with USCIS where they can update data as needed, where they can apply for benefits and where they can look and verify status of those requests. And to provide a single case management system for USCIS which will help in our overall efficiency. This is going to be a process that we deploy over time in a service-oriented architecture way, meaning that we're not looking atone monolithic system, we're looking at a suite of services that will enable our business process and we will probably spend between now and 2013 to fully deploy. We'll deploy incrementally and I'll talk about those increments in a minute.

Throughout the transformation process we will be looking at operationalizing privacy through compliance, to make sure that USCIS is fully compliant with statutory privacy requirements, ensure that the USCIS Privacy Act Office is actively engaged in all of our efforts to ensure that the tenets of the Privacy Act are built into the programs and to ensure that there's transparency about the types of information and the uses of those information by USCIS. Additionally, the Transformation Program Office has committed to an increased amount of education around privacy, to establish lines of communication between USCIS personnel and the Privacy Office via privacy training programs, to conduct workshops to raise awareness, to make sure that things are built and designed in compliance with those requirements. Currently USCIS has invested in three core capabilities for transformation: digital records which will be talked about by our Office of Records Services in a little bit, but essentially that is a move, the beginning of the move from paper to paperless sharing of A file or applicant administrative file data and information. More secure and better usage of biometrics, biometric storage. Currently we store 10 fingerprint images as well as some other biographic data such as facial image on many of our applicants. We don't have the capability right now to essentially reuse that information. If the time period lapses, we end up sending people back to application support centers for recapture. So from a customer service standpoint and operational efficiency standpoint customers would no longer need to be called back in. Also on that, from a national security perspective or simply an integrity perspective you lessen the likelihood of imposters or identity theft when you only capture the data once. And perhaps the most significant pilot with respect to privacy and security is the enumeration pilot where we will be linking biometrics to biographic data and managing the identity of an individual throughout the process. We will be able to - once we enroll them as we take fingerprints required for benefits as currently stipulated we will permanently link those biometrics images to the biographic encounter information. Whenever we encounter that individual again, we will verify biometrically who they are to make sure that they are the same person throughout the process.

We believe that a transformed electronic system will advantage our customers in that we will be able to extend our customer service to email notifications for upcoming deadlines, renewals, document submission, et cetera. We will have increased transparency of the business process and case status information. The ability to update personal account information with a change of address or a name change or the addition of additional information will be much easier in a web environment. Standardized business processes and a customer-centric environment. We'll be able to manage our customers' expectations better and be able to deliver on those expectations. As I mentioned earlier, we'll be able to reduce the amount of requests for duplicative information so we get the information from the identification once, it is in their account and then each time we need to refer to them again we can refer to that information

without requesting it again. We simply need to stop meeting the same person for the first time again and again and again. And we believe that we will have improved accuracy, consistency and efficiency through better metrics, better monitoring agency-wide. We will be deploying transformation in a, really a 5-increment manner, Increment zero if you will being these initial core capability pilots. To enable those pilots we are putting a - we are building a prototype case management system for the intercountry adoption cases. It's a fairly small workload, about 25,000 of these per year, but currently a workload that is not tracked in any national system. So we are securing that information. And again, the information about - the ability of manage identities of prospective adoptive parents, the ability to make sure that the child's interests are at heart the whole time makes this in my mind an ideal pilot for this process. In that process we will be deploying and testing the advantages and disadvantages, the limitations if you will of the biometric storage capability that we'll be building, enumeration, how that fits into our business process as well as the use of digital files to bring information to the adjudicator much more quickly.

The first increment which we'll be deploying we anticipate in 2008 will be the citizenship increment which primarily is the naturalization cases. And the remaining increments will generally follow in I guess reverse lifecycle from immigrant to - I'm sorry, from citizenship to immigrant petitions, those people wishing to live and work here for the rest of their lives, humanitarian and then finally non-immigrant status such as workers, visitors, students, et cetera. As I said we believe that this is - in this incremental plan we will be complete - we will complete enrollment by 2013. It is not a fast process. It is not an easy process. As part of what we're going to do we're not just taking the current immigration process and automating it. We're looking at reinvention, simplification, streamlining the process as we move ahead. The interesting thing is that as we deploy these new tools, these new capabilities, it is the same tools and capabilities that will help us deter and detect fraud that we will use to help identify those individuals who are low-risk and eligible. And it'll be those same tools that help speed the process for those folks. When you introduced me sir you talked about the IT transformation. This is not an IT transformation, this is not a business transformation. We believe that this is a performance-based transformation. We are looking first to envision what it is the agency wants to become, what metrics, what goals, what performance measures do we want to meet and then building business processes enabled with technology around those goals. So we have tried the business- driven transformation in the past. We have tried the IT-driven transformation in the past. Neither one has worked out terribly well. We are taking a performance-driven transformation initiative at this point and we believe that by 2013 and certainly you know by 2008 and then 2010, 11 and 13 we will be incrementally successful. Thank you.

MR. BEALES: All right, thank you. Ms. Ratliff.

MS. RATLIFF: Hi. I'm very excited to be here today to tell you about the two programs I'm overseeing through the Verification Division. I do have a handout and for those of you who like me need glasses to see small print we brought a few copies with the bigger slides and I hope you'll be able to look on and actually be able to follow along, especially with some of the screen shots we have so you can actually see what I'm going to be talking about.

The first program I want to mention has been called the SAVE program. Systematic Alien Verification for Entitlement is not a very snappy name, but basically what it does is for over 200federal, state and local benefit-granting agencies it is a way that they can electronically verify a benefit applicant's non-citizen status when that person is a non-citizen. So most of them are mandated by various laws to use the system and it's been in different forms for almost 20 years actually, starting with a paper-based verification and moving now to mostly an automated verification. Our biggest users are agencies like the Social Security Administration. So if a non-citizen goes into SSA to apply for SSI or even for a Social Security number before - they are anon-citizen, they say they're a non-citizen. Before SSA will adjudicate that application they'll electronically verify with us that that person is in fact in the non-citizen status that person described. And then we don't see therefore the person is eligible or not for any particular benefit, we're just verifying a status and then the particular agency will translate that information in terms of its own eligibility criteria for the particular benefit into you know what does that mean for their purpose. Last year we received about 10 million of those kinds of queries and so right now it's the bigger program of the two that we work on in the Verification Division. But the program that really gets all the attention lately is a program that has been called the basic pilot which again is a nondescript name for what it does, but it's a program that verifies the employment eligibility status of both in this case citizens and non-citizen new hires. So new employees of workers, of employers who are choosing to take this extra step. All employers - when each of you got your job, unless you're self-employed you should have filled out a paper form called the I-9 and that's been the law for 20 years and it comes in the pile of papers your first day that you know, you may not even remember filling it out. But it's a form that every new hire has to fill out and you show a document that establishes who you are and whether you are work authorized as a part of that. And so for citizens you would show typically your passport or a driver's license and your Social Security card for example. Non-citizens have different choices of documents that they can show. So that's the law for all employers, but because it doesn't have an electronic verification piece to it, about 10 years ago Congress authorized a pilot for employers who want to take this extra step. And over the years interest in it has been growing slowly. The drumbeat has been increasing move and more over the last year or so. Right now we're getting about 50 more employers per day signing up for it. And we've been calling it EEV for Employment Eligibility Verification to try to describe to

people who haven't heard about it yet a little bit about what it is. So you're going to be hearing the phrase basic pilot less often and EEV more often as we try to do more and more outreach about what we're doing and how we're improving this year. So we've got as of a few weeks ago 15,000 employers voluntarily participating in EEV and about six months ago we were at about 10,000. So it's grown 50 percent just in the last six months. And based on some outreach plans that we have to try to get to more employer segments, who we think would be most receptive to participating in this voluntarily, we're hoping to see the rate of growth even expand beyond the current 50 a day to be a significant increase in employers who are willing to use this program to verify the work authorization of their new hires.

For the SAVE program really the most interesting thing going on in SAVE right now is REAL ID and I don't want to - I understand that was addressed by other speakers this morning and my program is a very, is a small piece of all of the pieces that are going on under the umbrella of REALID, but we would be the piece where for non- citizen driver's license applicants who come in to apply for a REAL ID license, we would be verifying not all of the information about them, but their non-citizen status. So for us it's important in terms of our planning, but for the big picture of REAL ID you know we understand we're a small part of that big picture. But we are planning to have our data fields and our processes tweaked to fit the DMV's needs and the REAL ID law's needs at the right time. We currently have20 DMVs participating voluntarily in the SAVE program, not in the REAL ID way, the REAL ID complete way. They are using it like our other users do and they -most of them use it more selectively, sort of as needed and so there would be some changes that we would make to make our system fit the REAL ID requirements at the right time.

For EEV, obviously the most interesting thing going on this year is getting ready for possible enactment of a mandatory program. Last year both houses of Congress in different larger packages passed provisions making EEV mandatory. The House passed it with a 5-year phase-in. The Senate passed it with a much more aggressive 18-month phase-in. And the appropriators gave us $114 million ahead of the law becoming - making the program mandatory to let us get ready. So we're trying to go this year from a program that really does an okay job doing what it needs to do to becoming a program that's A+, that does a great job doing what it needs to do for the current participating employers and then for the 7 million employers who would have to register, be trained, use our system correctly under a mandatory program. And it really is a wonderful position to be in to have a year. Congress with immigration issues doesn't often give money ahead of assignments so we're trying to really take advantage of this year to make the WebPages more user-friendly, to make our data as complete as possible so if a new hire is in fact work authorized, we can verify that instantly and the employer and the employee don't have to take any additional steps.

Right now we are evaluated independently by a company called West at, a research firm, and their latest report found that 93 percent of the new hire queries are verified as work authorized instantly. That was good news for us because some of the complaints that we get, really I would say the biggest complaint we get about the thought of making basic pilot - EEV mandatory is that if you go to 7 million employers which would be over 50 million queries a year, you can't have a mismatch rate that's going to crash the system even if it has to do with you know things that aren't really the fault of the government. You know we have some mismatches that occur because the person naturalized. They should have told SSA, but you know we don't all rush to take a day off of work to go down to SSA with our naturalization certificate as a priority. Well, if you don't do that and then you get a new job for a basic pilot employer and you say you're a citizen because you are a citizen, you're going to be a mismatch because SSA doesn't know you're a citizen. You haven't told them. So this will remind you need to take your certificate down to SSA. You have an interest in the SSA records being complete and up to date. So we do have types of mismatches that occur because the person has changed something about their information, but hasn't told the right source. The person got married and changed their name, but didn't tell SSA, for example. We are working behind the scenes to do all that we can to save mismatches from happening. For example we are working to see how we can get SSA information on naturalized citizens. You know, our agency knows the person was naturalized. We naturalized them. So if we could electronically get that information to SSA's Numident system the person doesn't need to take a day off of work to go into SSA with their certificate themselves. So we're trying to look at ways that we can address the issue of data being not complete due to you know the person not yet following through to provide the new information to the right source. We also have done three or four data projects this year, several are in production and the others are close to being in production, where we are making sure for non-citizens that our DHS data is as complete as it can be. We've got some cases just due to our own system, current system that Dan's straightening out over time of stovepiped databases that don't always talk to each other where we may have information that was right at one point about a person, but is no longer up to date. So we have been this year analyzing what are the sources of DHS mismatches that we could do something about again through linking to the database that houses extension of status and change of status information. So now we'll know a non-immigrant's latest status. That won't lead to a mismatch that then takes time to track down and sort out. We also are moving to a new query by card number method for non-citizens. And right now we query by what's called a number for Alien number or I-94 number which is an arrival number. And there can be times when due to different data issues and data entry issue someone had - there's a typo, they have more than one A number, et cetera. Well, but you only have one card which only has one card number on it so we've built a link to our card repository which houses information from our green cards for permanent residents and the employment

authorization documents which 80 percent of non-citizens when they get a new job for the Form I-9 they show one of those two cards. So we're beginning a pilot that actually just started this week with about 40 employers where instead of querying by A number or I-94 number and possibly leading to mismatches just due to our different stovepiped systems, they're now given the opportunity to query by card number when they've chosen to show a green card or an EAD for the I-9. And it's going to be a one to one match against that card repository so there will be no typo issue, there'll be no which A number was it issue. It'll be the card information we put on the card. And we are expecting to see a reduction in the number of queries that have a mismatch and have to go to a secondary manual verification stage based on this new process. And we're very excited to get the pilot a few more weeks under our belt so we can measure how much progress did we find.

Also with this query method we're going to be able to pull up the photo. This is the beginnings of a photo-based check, identity check. We will pull up the photo that should be on the green card or the employment authorization document. We know that because we're pulling it from the repository of that card information. So it's the photo we put on the card. So this will help with photo substitution fraud. So if the employee has shown the employer a really good forged document where they've put their own photo on someone else's green card for example, it'll be very easily detected because it will pop up on the screen - this is a web-based system - on the screen the photo that should be on the card. So this won't be a matter of oh, did he cut his hair, the shirt's different. It should be 100 percent the same photo. It should be the photo we put on the card. So again this is a pilot we've just launched this week with about 40 employers. We want to proceed carefully to make sure our procedures are clear, we understand what we're doing, employers understand, there's no unintended consequences. But we're very excited about the possibility of having potentially a very easy tool to detect photo substitution fraud.

As we move to begin to do more outreach to try to reach employers who we think will be most receptive to joining EEV, we're thinking about reaching out to some critical infrastructure sectors who likely would be interested in doing an additional step to verify identity. We are already being contacted by many, many employers in some states that have passed state laws that promote the use of EEV, Georgia and Colorado being the biggest. And we're also reaching out to HR professional type groups who are - their business is the hiring process. They're very interested in staying on top of the latest technology and programs that are out there to expedite the hiring process. And we are - a big priority for us this year is to work with employers and say look, it's voluntary, you don't have to use this, but if you will do it just to put your toe in the water and then give us feedback we can make the process better this year before it becomes mandatory. Once the law is passed making it mandatory there won't be as much time to be making little tweaks and improvements. We're just going to be probably surviving just trying to register employers and get the system up to speed. So this is the year to make it go from

not an A program, maybe a B program, to an A+ program. And we are finding that employers are very interested in working with us.

In terms of the system behind EEV and SAVE, behind both systems, it's called the Verification Information System, VIS. And so the same database is used to verify non-citizen status for both the EEV front end and the SAVE front end. It currently holds records from our central index system. Just recently we began - I described some - we're doing some data completeness projects. One of them is to add information from our agency database called CLAIMS 3 that houses non-immigrant information. So that's where we're getting extension and change of status information. The query by card method is using a database called ISRS that houses the card information. And we have been getting for years an extract of TEX IBIS arrival information. This is information that is data-entered by a CBP, Customs and Border Protection contractor and because it's data-entered after the fact there's often a several week delay in the information getting into their system and then the next day into our system. So we've been very interested in getting more immediate arrival information and as of last year inspectors are entering arrival information real time into another part of TEX IBIS based on the advance passenger information system. And we have just finished reaching an agreement with CBP to get access to that information. So now someone who got off a plane and started to work the next day for an EEV employer, you know a few weeks ago we wouldn't know that they were in a legal status yet because CBP had to data-enter it and then we would get it the next day, maybe two weeks later. But now we will get that information the next day through this real time - the real time system that we've just reached an agreement to receive.

So who do we let use our system? On the SAVE side, agencies have to sign an MOU with us. It's reviewed by our counsel office. They have to have a legal hook to use it, a law that authorizes them to electronically verify a non-citizen's status. On the employer side, really any employer can volunteer to use EEV. We are looking at adding some identity verification features to try to be rigorous in who we are allowing to use our system. Right now a company executive typically will sign up for the system and then allow their HR specialist to sign up who actually will be running the queries, or if it's a very small company it could be the same person. But typically you have a corporate administrator role and then several HR specialists who actually are interfacing with the new hires. And we are looking at adding an employer EIN verification piece and even a user SSN verification just to be able to bring some rigor to who is signing up, are they who they say they are, before we let them use our system.

I've mentioned the databases that are in VIS. We also have access to the SSA Numident database. We don't receive an extract of it into our database. We ping against it when a - for the EEV program to verify SSN information. The thing I was most

interested in you being able to see big and not too, too tiny was the screenshots of what the EEV system looks like. It basically uses information from the Form I-9, so we're not collecting any data that's additional over the requirements of the law for the Form I- 9. I would love to be in a room that had internet access so I could just quickly show you. Basically we'll take your last name, your first name, your date of birth, your Social Security number, your hire date because this query is supposed to be run within three days of you starting for work, your citizen status. If you're not a citizen we take your A number or I-94 number for the non-citizen check. We capture the document type which means the document you showed for the I-9, your identity document, and that's information that all comes off the Form I-9. Then typically within one to three seconds the employer is going to get back a response. Ninety-three percent of the time what they get back says work authorized. Within those one to three seconds the system has gone into Numident, the SSA database for SSNs, verified name, date of birth and SSN. And if the person attested to be a citizen we rely on SSA's records of citizenship. If the person attested to be anon-citizen, after we verify their SSN through Numident it will then go into the DHS side - into VIS and verify that they're in a work authorized non-citizen status. So that happens in one to three seconds. If we cannot verify the information, the employer gets back what's called a tentative non-confirmation. And I included one example of an SSA tentative non- confirmation. In this case the SSN was invalid. In that case the employer notifies the employee that there was a mismatch. The employer can contest it and say I don't know what you're talking about, I've had this SSN for 45 years, here it is on my card. That's fine. The person cannot be fired or have any adverse consequences during this sort of yellow light stage. They have eight days to go into SSA and work out the problem. And typically they can work it out at the front counter that day and then the employer will re-query the next day and then should get a work authorized message. There's a similar process for DHS mismatches, and I know I'm talking too long so I don't want to go into too much detail, but we do an extra check behind the scenes of our records and then issue a tentative non-confirmation in a similar way. For DHS mismatches they don't have to visit us in person. They can call a toll-free number. And we typically resolve those mismatches in three days.

You have a screen that shows what employment authorized looks like and the employer would just write down the case verification number on the Form I-9 or print this screen and that's all they have to do. So for 93 percent of their new hires it takes, the whole process might take a minute or less depending on how quickly that HR specialist types in the information. Another thing I just wanted to quickly mention because it does go to how we're trying to be aware of privacy concerns is developing and monitoring a compliance function this year. We are right now in the stage of beginning to write an SOP so what will our monitors and compliance staff actually do eight hours a day. But at a high level they're going to be looking for systematic evidence of employer misuse of the

system. If an HR specialist is essentially fishing, like hmm, you know I don't have any new hires to process today, but let me just try to query my neighbor, or my friends, or keep spelling a name differently to break the algorithm for verification. We'll be able to see that and take follow-up action, perhaps calling that person or their supervisor to say you know in a voluntary world we're going to terminate your use. In a mandatory world we likely wouldn't be able to, but just to call that kind of misbehavior to the employer's attention. We'll also be able to see if possible evidence of discrimination, for example if an employer is only verifying non-citizens and there's been enough time go by and the size of the company is such that they've hired enough people that statistically there generally would be citizens in their workforce we can easily see that in the system by monitoring and then perhaps call the employer and say have you forgotten this is for citizens and non- citizens. You know it's not a tool just for non-citizens. Or if they sign up and don't run any queries we could say have you forgotten you know that you're a part of this system. And we are working closely with the DHS Civil Rights and Civil Liberties Office to make sure the SOP on monitoring and compliance is complete and looks for privacy concerns, civil rights concerns as well as enforcement or fraud type concerns.

We are doing a lot of hiring this year to help us do all the work to improve the programs. I've mentioned the photo screening tool which is basically our latest functionality that we're working on to pop up the photo that should be on the green card or the EAD and that obviously has a wider applicability to down the road perhaps being able to get access to other photos that an employee might be showing for the Form I-9. But this is really a functionality in its infancy stage. And we are currently uploading into our database the green card photos, the EAD photos and that's like 17 million photos so we have a ways to go even to get that phase of this functionality completed.

The last screenshot shows the photo tool message when the person is work authorized and it will display the photo that should be on the card the person used for the Form I-9. And that photo can be enlarged. It's actually very good quality photo. And then the last page of the handout is just my email address for any potentially future questions and we always - always in the marketing mode. We always include the employer registration site for EEV and it's interesting even just to go into the site and look at the data that we're asking for sign-up. And it's a paperless sign-up for the employer. So thank you very much.

MR. BEALES: Thank you. Neville Pattinson.

MR. PATTINSON: Thank you. Very interesting. I'd like to ask a few questions to Mr. Renaud on the digitization process and paperless transformation. Is the program retrospective on the 100 million A files or is it something you're starting from a day coming along and moving forward? That's the first part of the question. Maybe you could answer that first and then I could ask the next piece.

MR. RENAUD: Thank you for the question and I think the answer is yes and no. Currently we are scanning A files to be put in the electronic repository and then have access to digitally in a proactive manner. And what I mean by that is we have identified files that will be used to support our first electronic end-to-end processes. So those we have pulled from our shelves if you will and we are scanning those. That combined with the beginning of electronic intake will be what builds our electronic repository. We do not have an interest, a need or I talked about efficiency. It would not be terribly efficient to scan 100 million A files when we probably only really need you know a small percentage of those long-term. So we're trying to go about it as smartly as possible, trying to identify those cases that we will need for those lines of business that we are going to automate first.

MR. PATTINSON: Thank you. Second part is on the reference to the PIA that's been presented to us in advance on this subject. And it talks about whether you'll be scanning the A files. Is the access to that A file entirely available, every item in the A file once it's scanned, or are elements of the A file protected selectively? Is it going to be all or nothing approach?

MR. RENAUD: Right now and I'm going to do what Dominick Gentile always does to me and say that's a question for Records. But my understanding is it will be roles-based authorization or access to the file. Right now the - I know that there's some files, some are classified, some have other security or privacy ramifications to them. Those we are not scanning right now. Immediately the ones that we are scanning we will have - those who have access to the system will have access to the entire file. Down the road we do look at roles-based access where someone would need a certain clearance or a certain need in order to access certain data. And hang on, let me just look behind and see if Dominick's nodding in the right direction. Yes, that's correct. Thank you.

MR. PATTINSON: Great. And the last part, just to monopolize the questions a little bit. The green card itself is part of the process. I'm not sure your remit is to go that far, but you talked about securing biometrics and improving how that's dealt with and putting through a biometric tie to the biographical information. The green card has the fingerprint printed on the front of the card for a permanent resident along with their photograph. Is that still going to be a practice adopted, or are we going to be looking at being a bit more privacy sensitive to biometric information on the card itself?

MR. RENAUD: I think even if the answer were no I'd say yes, but - in this forum. But I do think that as part of our second increment which is the immigrant increment we are going to be looking at what type of evidence of permanent residence or employment authorization or whatever status that we care to document is most appropriate and what needs to be on that card. Currently we have a fingerprint on the card as you note which frankly I'm not aware that anyone has ever really used to identify an individual. Similarly

we have a signature which I believe also we don't. What we envision long-term is the card simply being - or frankly a biometric being a primary key to a database that would return certain information. And so in that regard I would say that we would - you could effect the same thing with essentially a blank card that just acts as a key. So we are going to take a hard look and I think we will, you know in that process we will reach out hopefully to this board, certainly DHS Privacy Office to figure out what is the best way to meet our business needs while protecting the privacy of our customers.

MR. BEALES: Mary?

MS. DEROSA: Yes, I'd just like to maybe hear a little bit more about - on the EEV program about the monitoring and compliance function and whether the idea is to - assuming you will have audit logs, how regularly will they be - how will they be monitored and will there be automated analysis done or is the idea to have it all manual?

MS. RATLIFF: We very much are in the beginning stages, so I would say we're open to suggestions and feedback. We are really just beginning to sit down and brainstorm those type of issues and I think I see on periodic reports being run and then looked at by analysts. To the extent that it can be automated that's useful so that our analysts are focusing on the things that they need to focus on. But the type of things we're thinking of right now are you know from the very innocuous, employers who aren't closing cases out, that reports could be run that just indicate queries that never got a final closure code, you know. We want employers to do the system properly, you know even to that point of the final step. Things like, we'd be able to see things like multiple SSNs, duplicate - SSNs that have been used multiple times that don't suggest I had several part-time jobs. I mean, for example we recently just did an internal analysis just to see what is there to inform this program development and we saw one SSN that had been run like 50 times so we thought well that's interesting. That could be document fraud, vendors selling someone's identity, or it turned out that it looked like it was one HR user fishing. Sort of oh if I spell Gerri with a G, ding, work authorized. I think I'll spell Gerri with a J and see what happens. Oh, it didn't - non-confirmation. You know you could see it was one person playing over about an hour. But - which is in a way not good, but in a way it was sort of - it was a relief that it was one person being inappropriate, not document identity theft or something. But I think what we intend to do is brainstorm lists of types of reports like incomplete queries, multiple SSNs, multiple A numbers in patterns that don't suggest several part-time jobs, employers who have never used the system, sort of the examples I was giving to have those kind of reports generated periodically. But I mean we would certainly welcome feedback on what you feel is an appropriate way to proceed and the efficient way to proceed because this is just - it's in its infancy to try to develop this function.

MS. DEROSA: Thank you.

MR. BEALES: Jim Harper. .

MR. HARPER: Thank you both for being here and informing us about your work. Appreciate it. I wanted to understand Ms. Ratliff the relationship between what you do and the national new hires database. Is that a different project somewhere else, or is that something you're involved with?

MS. RATLIFF: Is that the child support database?

MR. HARPER: I think it's used for that, yes. I don't know what the original use for it was. Do you share information with someone else?

MS. RATLIFF: We do not. We do not. I have heard of it and just trying to learn what's out there. I think that's used for child support purposes, but we have not talked to that program. We don't share information with that program. .

MR. HARPER: Do you have any idea where they would get their information other than from you? I don't know if employers being required to -

MS. RATLIFF: I think they - I should say let me research it and get back to you. I think it has to do with either like state tax reporting type context where that's gleaned from. That's my sense.

MR. HARPER: Okay. I was also curious, the - you've got a number of employers signing up with you voluntarily at this point. What's their incentive to do that? It's obviously not for their health.

MS. RATLIFF: They have different incentives, different employers. Some of them are in industries that have recently had a work site enforcement action and so they are interested to do anything extra to innoculate themselves in their perception against getting an action initiated or do all that they can to not have an issue if they do have a work site audit. There are some who honestly seem to think it's you know their duty to go above and beyond the law's minimum to have an authorized workforce. There are some who live in states like Colorado and Georgia who think my state law is requiring me to sign up so I will. There really do seems to be different motivations. There are some who like the fact that it will immediately surface an SSN mismatch because our enforcement sister agency ICE, they are doing some rulemaking around looking at companies with I think it's a hundred or more SSN mismatch letters, that that would inform work site enforcement actions. So companies are realizing through EEV if there's a mismatch for your new hire you're going to know it in a second, the new hire is going to resolve it or you can terminate them. So that, we get a lot of questions about that, that you can tell they're worried about that mismatch. So they're - it's an enforcement inoculation. Frankly I always try to mention in my presentations this isn't an enforcement tool, it's a neutral information-sharing program. And I hope it also helps employers avoid the temptation to discriminate because it takes the burden off looking at the card and

worrying is this a really good forgery. And so if you are a work authorized person, you're going to verify and you don't need to worry about the employer being tempted to discriminate against you. The employer doesn't have to worry about being a document expert. It just really makes the document itself less important because we're going to verify behind the scenes.

MR. HARPER: Just a brief follow-up if there's a little leisure. I guess inspired by the new hires database I wonder if your system would preserve records of people being hired so that it proceeds a similar information source to agencies. For example, if someone is going to one agency claiming entitlement to benefits and you have information showing that they were recently hired to a new job that would prevent them you know being eligible for benefits. You could be a similar type information source. I assume you keep the data about usage so that you would be such a source?

MS. RATLIFF: Our data retention period is five years right now. And I mean I think sure, operationally from an IT perspective we could do what you're suggesting. I mean obviously it would be a policy call about is that appropriate, but I think it's true, especially with things happening on the Hill like looking at a temporary worker program where it could be that workers would need to document quarters of authorized status, that people have begun looking at EEV with an eye toward could you collect more data, could you record not only when the person has started the job, but when they have left the job. So eventually you could piece together. There's some provisions on the Hill where SSA would have to or maybe not literally legislative provisions yet, but discussions about requiring SSA to verify that their Social Security applicants had - each qualifying quarter was in a work authorized status, not just - I think currently the rule is one of them had to be to count. And so we are getting questions and expectations are out there about could we do more. But I mean I think there's an IT answer, of course we could do more, and a policy answer about what should we do. But right now we have no plans to do more than try to do a great job at what we're doing.

MR. BEALES: We have time for one more question. John Sabo.

MR. SABO: Thank you. Just a quick question on the link to the Numident at SSA. It says you receive no data fees. I presume you mean you don't get data fields, you're getting an indicator code back, yes/no, or?

MS. RATLIFF: We get codes that we translate through decision tables.

MR. SABO: Right, okay. The other thing was the issue of non - in terms of compliance and the kind of monitoring you're looking for abuse. Is this Numident linkage a batch link or is it a live linkage?

MS. RATLIFF: I believe it's correct to say it's a live - it's query by query, so.

MR. SABO: Because SSA itself has algorithms in place to look for excessive use of a particular query against a particular number, that type of thing. And the comment you made about somebody entering G and a J, there's also tolerances because the SSA database includes data of varying quality. And I'm assuming you've had those discussions with them about the fact that –

MS. RATLIFF: Yes.

MR. SABO: So I guess you're looking for some leads on monitoring and compliance. It could be very well that SSA could provide some of that for you. I guess you'd have to pay for the programming, but they're already capable of doing much of that."

MS. RATLIFF: Yes. Yes, thank you.

MR. BEALES: All right, well thank you very much. We appreciate you being with us today. Our last panel will address Data Integrity and Records Retention Within DHS. We will be joined by Dominick Gentile who's the Director of Records Services at CIS. He was selected as the director in 2000 and he is responsible for the Office of Records Management for the National Records Center for Freedom of Information and Privacy Act and also for Records Systems Services. He is also a shared service provider servicing Immigration and Customs Enforcement and Customs and Border Protection. We're also joined by Kathy Schultz who's a Senior Records Officer in the Records Division in Department of Homeland Security. She's been with DHS since the beginning and was initially managing seven programs by herself, Records Management, Forms Management, directives, printing, library, FOIA and Paperwork Reduction Act. Sounded like a busy day. Previously she was the senior records officer for the Department of the Treasury, an appraisal archivist at the National Archives and a records officer at the Patent Trademark Office. Welcome to both of you. We look forward to hearing from you.

MR. GENTILE: Good afternoon. As Dan Renaud had mentioned, digitization is a small piece of the overall transformation project and today I'm going to talk to you just a little bit about our facility in Williamsburg, Kentucky, talk a little bit about some of our records systems, and also kind of the A file management. As Dan said, we have over 100 million files that are paper-based files and two records series. That's our A file series and our receipt file series. We also have about 60 to 65 million historical files that are digitized in one manner or another or in paper. So we do have an enormous amount of paper that we deal with. And what we've done is when 9/11 happened we were given 19 names and information about those 19 people and we spent the next three days searching all through our data systems and we came up with about 3,000 to 5,000 files that may or may not have been related to the terrorists. Now unfortunately they were in a cave in Missouri and if someone wanted to see them they had to get on a plane and fly out there because we locked them down. So as part of the 9/11 Commission the Congress actually gave us

money for the first time. This is our third attempt at doing electronic A files. So we actually have money and transformation working with us. And we are the beginning of the transformation piece for USCIS. And we also, as you said we support ICE and CBP so part of the sharing is to allow ICE and CBP as well as DHS and other people that actually need access to the files to be able to view the files. In our facility in Williamsburg, Kentucky we have - the contractor actually runs and manages that site for us, the CSC-Datatrac. And we have about 560,000 files at the center. Of the files, we've already scanned at least 300,000 of the files and we're going through a QA process. There's about 244 contractors on board. Now the contractor does a very high QC check on those files and we actually have another contract, Labot that's working with this contractor where we have about six contractors, QA contractors and actually two government workers who are going to be on board as of April. We are rotating people in from my office and from the field. We're doing 100 percent quality assurance during the pilot phase. We do multiple reviews. We do an initial triage. We do a systems check. And then we check the image quality as well as meta data and image compression. One of the interesting things we've found is that the actual scanning of the file and indexing and OCR'ing it is not that expensive. It's taking the file apart, and for some reason our adjudicators love to staple and they put about a thousand staples in one document. So we're actually trying to figure out a way to recycle staples and come up with a way to sell back furniture or some kind of thing. The amount of money we spend taking the file apart and putting it back together is where the - so for instance if it's $10 to scan the file, at least $8 of it is taking the file apart and putting it back together, about $2 to actually do the scanning. So that's what we're doing in Williamsburg and that's the first piece of what we're doing in support of transformation.

The question came up are we going to go back and do all the files and the answer is definitely no. What we're doing to do is what we call scan on demand or request. If we get a request for a file we hope to bring that file into the digitization process and part of the FY '08, by FY '08 we have to come up with a plan to support ICE and CBP electronically. So we are working on ways of doing that. Kind of a little bit about records systems because it ties into what we're doing with the paper. We have several records systems. One's our national file- tracking system. We track those 100 million files throughout the whole United States and actually overseas. So I can tell you where a file is, if the system has been used correctly, to a foot of where that file is anywhere in the United States. We have the National Records Center who maintains about 24 million of the paper files and right across the street at our Federal Records Center in Lee's Summit, Missouri we have another 22 million files. What I can't tell you is what's in the file. I can tell you where the file has been, I can tell you where the file is at, I can tell you who had the file last, but I can't tell you exactly what's in the file. With the new digitization process we're doing an indexing and OCR of that file so it's sort of like when you first open up a

table of contents it'll tell you every document that's in the file. We are scanning every document and we're labeling mainly around form type or significant information like marriage certificate, divorce decree, any type of - birth certificate, things of that nature we actually label so an adjudicator can look into the file, the first page and go directly to a document they need to look at. And then their supporting document would be at the bottom of the page. We also are working on notes so we could put notes on the file if there's some issue. Adjudicators love to put things in files. Paper files, we've found skateboards, we've found peanut butter and jelly sandwich, we found gum. It's just incredible what goes in. I guess if you don't know what do with something you put it in a file. And I think that Kathy will be talking a little bit about what we're going to do with some of those things. So we work very close with DHS. It's amazing the amount of files that we have and we're creating 1.2 to 1.6 million files a year, so we're hoping Transformation gets out in front of us and we stop creating files and we just go to an electronic medium where we no longer have to create paper files.

We also have a system called MIDAS which is Microfilm Digitization System that we've actually taken old microfilm and we've digitized and put it on a new web - we're actually going to web-enable it so everyone in USCIS will - excuse me, and ICE and CBP will have access to that. We established MOUs with the other agencies. As I said earlier we do support ICE and CBP for their records piece of it. We all share the A file, but USCIS is ultimately responsible for the A file. We are - to help with data integrity and data issues that we have, back probably in 1986 the decision was made to not put certain data in our systems. It was older data and we've since found that that was probably a mistake because now people are coming up and actually Gerri Ratliff's team is dealing with people applying for benefits and we don't have that information in our systems. So we have to go back to the Federal Records Center. We're doing a lot of what we call data compaction and data integrity checks where we're calling back old files, we're going through the boxes of the files, we're updating our system, cleaning up the files, bar coding and then returning back to the Federal Records Center which gives us a much better kind of audit of our files and is also going to help us determine which fields we actually send to the digitization facility.

We are working very closely with NARA to schedule the system. That's the system Dan's creating for us. What we do is the front end processing and digitizing of the files and then we will post them to a system that Dan and his team are working with. We are actually part of that team, but Dan has the overall responsibility. And as he was joking when I go out and speak about this, all of questions come up about retention or are you going to be able to see the file this way or this way, and I always punt those questions to Dan so he was happy to punt a few questions my way. We are also looking at conducting a complete review of all the systems that we have now and all of our retention schedules because at some point we're going to have kind of three things going on. We're going to

have paper, we're going to have digital images of the paper and then completely digital. So we're going to have to have several different retention schedules to address all the different variations of the file. So we are working close with Kathy and with NARA.

We have a couple things that are coming up this year. We're working with the Law Enforcement Service Center in Burlington, Vermont. They house about 350,000 files that deal with - they're A files that deal with absconders. We are looking at digitizing those so ICE will have access, immediate access to that information. And also ICE - excuse me, CBP and USCIS will have access to that too. We're also looking at expanding the national file tracking system to three of our larger service centers and then that will encompass all the offices that we have so we can have a better data quality and track the files and the information a lot better. And we're also working with the training facility down in FLETC to institute a training class for all of our adjudicators that deals with FOIA, records and records retention. We're kind of moving, if you can imagine a circle with a little bull's eye in it, that's where we're at now. There's over a million files and we're estimating we have about enough funding to do you know just - or excuse me 100 million. We have just about enough money to do a million files, so we're being very selective on what those files are and we're working very closely with ICE, CBP and our USCIS adjudicators to figure out what to target and what the best payoff is for that."

MR. BEALES: All right, thank you very much. Kathy Schultz.

MS. SCHULTZ: Good afternoon. It's an honor and a pleasure to be here today and I know Hugo is not in the room, but I wanted to thank him for all of his support for DHS Records Management and to his staff for their good working relationship on privacy and records issues. It has helped me tremendously.

To get to the heart of the matter, Records Management is governed by the Federal Records Act which was passed in 1950. Before that there was not an organized method for dealing with federal records. Some things of value were thrown away and other things of no consequence were saved. So the Federal Records Act established how federal records would be maintained. In that Act it spells out that every agency must have a records management program, must have a records officer, retention schedules for federal records, training program, et cetera. These are requirements. And starting at DHS in the beginning there was nothing. So we've been working now for four years and are on our way to getting the retention schedules established for DHS headquarters. And I have been working with the records officers and the components to do the same thing, as Dominick mentioned. He's a specialist with A files and I'm a general practitioner with records management in general. I do work with the different components at DHS, but my concentration for active scheduling is at headquarters. The Federal Records Act and the mandates it imposes promotes the smooth operation of government. It protects records from inappropriate access or destruction, ensures accountability to the Administration,

Congress, the courts and the public. It is important to DHS because it's the law. We want to abide by the law. We want to preserve the history of the department and protect the rights and interests of the department and the public, and protect the financial integrity of DHS. We're all accountable in some way or another and our records show how we've spent our money and the decisions we've made. And as you can see, there's a statutory definition of a record and it's essentially anything made or received in the course of business. Hugo and I have a difference of opinion on what's a record. I say everything's a record, but they have different values. He wants to tell people what they can throw away. I tell people what they should save. So but all in all we agree that records are important. In order to have an authorized disposition for a record we go through a scheduling process and that involves going to a program area, talking to the person that runs the program, asking them what they do and what records come out of those activities. We take into consideration the level of the office within the department, what regulations govern that program. Is there something in the Homeland Security Act that governs the program. And what is the business need for the record over time. If it's something that deals with benefits we would want to make sure that we're maintaining that record to promote that benefit over time. So as I have said, we are scheduling records to provide an authorized disposition and basically there - I know this is basic records management, but just to give you an idea of what the program is about. There are different types of records, and I mentioned program records for mission- related activities. Administrative records are kind of what everybody has behind the scenes, time and attendance, payroll, that type of, personnel. Non-records are, even though it says excluded from the legal definition, generally if it's a copy of something that's kept purely for convenience. It has no value to you other than reference. That's anon-record. And magazines, books, that type of thing and personal papers. I always mention this in briefings because even though we're not supposed to keep personal things at work, we do. So we address that. And the federal government owns federal records, individuals don't. Even if they are working on something they can't automatically take it with them when they leave. They have to ask permission.

And the schedules are comprised of a description of the record, what it is, how it's used and the schedule will say when something can be deleted or destroyed or transferred to the National Archives if it's permanent. And every agency is required to create schedules to cover all of its records. And the mission-related schedules have to be approved by the National Archives.

I am only going to touch briefly on electronic records. They can be in any media you know that's machine-readable. The same rules apply for retention as it does for paper. We try to make some of our schedules media-neutral. So if you have a paper copy and an electronic copy, you decide which is the record copy and you follow the disposition instructions. And electronic records are being used more and more in the

courts as evidence so consequently they must be authentic, accurate and trustworthy. We have to make sure - ensure that security procedures prevent unauthorized addition, modification, or deletion of the record. And it is a challenge. And we do work with legal staff in coordinating those procedures and policies. We do use the same standards for electronic records as we do paper. They must be maintained and easily retrievable. And with electronic records if people use a file plan and index them or label them properly they're much easier to retrieve. There is a slide on email records and it's basically saying the same thing it says for paper. It's talking about records, not paper or electronic, but records. And emails are records. And many people like to lump them together and say what do I do with my emails. How long do I keep my emails. They're like any other record. They're on different subjects. So you have to look at them by their value by subject rather than the media, that they're an email. They can provide, as this one slide mentions, they can provide comments on a draft action memorandum if the email message is necessary for proper understanding of the context of the action. If a decision is made or a memo is written and the email sending it forward explains it, you should keep the email. Messages providing documentation of significant DHS decisions and commitments not otherwise documented in DHS files. Some people write emails after they've had a discussion with someone to verify or clarify what they've discussed. That is a record. And so the question comes up how do we manage these electronic records? And it's a very good question and one that the government has been dealing with for many years now. The Department of Defense set up a standard for electronic records management systems. It's called DoD 5015.2. They test systems against this standard and the government agencies are expected to use this standard when looking at or implementing a records management system. The disposition schedules go into the system. Records are tied to their disposition in one of these systems. And at DHS currently there is no system for managing electronic records. However, we are piloting a system at this time right now and it's going well except we're going through those hurdles that you have to jump to get a system implemented. So we haven't actually flipped the switch for the pilot users to be able to use the system. We've had some testing, but we have not implemented the pilot yet. And the benefits for an electronic system is that you meet the mandates of the federal laws and you are able to abide by your disposition schedules for electronic records. You can facilitate document and information sharing and access to records more easily. Faster responses for FOIA and requests from Congress. And it eliminates keeping paper copies just in case. We are utilizing a file plan based on the federal enterprise architecture lines of business which designates records by function rather than organization. And we have had some reorganizations since we started so this makes it much easier for us. The - within the system users are assigned a maximum security level by an administrator when their account is created. Each record is assigned a security level either through the file plan folder or individual record by document originator. In other words, you have access to your records, but you don't necessarily

have access to others' records unless you are in a group that shares records. That's part of the security in the system. And we're very happy to have that.

Each user may be assigned to a user group. People who work together such as in the Records Management Office would be in the same group. If I had something in particular that was confidential or classified which I don't, I could see those records only. I would have a special account where no one else would have access. So that provides privacy and security. And assignments are controlled at the administrator level.

I know I went through that very quickly, especially about electronic records, but I wanted you to know that we are working on this issue for security and privacy of electronic record storage and I know we'd both be happy to answer any questions you have.

MR. BEALES: Well thank you very much. Neville Pattinson.

MR. PATTINSON: Thank you very much both for your very interesting information. I think Dominick Gentile got off lightly because I asked my questions to Mr. Renaud earlier. So to address the question to Kathy Schultz, regarding the integrity of records, I hear a lot about the retention of records, the putting them away and storing them and keeping them and having a policy and so on. But how do we know that they're being maintained with integrity and they're not being eroded, tampered with, modified and so on? And I think you answered the second part of my question which was about security and access on the last couple of slides so I got ahead of myself on my question, but perhaps you could answer me about the verifying the integrity of records.

MS. SCHULTZ: Paper records? I mean we're working towards that on electronic records. We aren't there yet so I can't guarantee the integrity. We do have safeguards in some areas. Classified systems are not on a common server. Classified records are handled entirely differently. The only involvement I have at this time is talking to people about the content of the record as far as the business relation of the record to the DHS mission, not exactly what is in each record. So there is a - the areas that do have classified records do safeguard them. You have to have certain security clearances. They have - I think you've probably seen where when you come onto a floor where they have classified records or classified systems, the red light goes on and anyone without the proper clearance has to be escorted and the red light stays on while they're on the floor. So there are programs within DHS that ensure the integrity of those types of records.

Other records we have to - we do some monitoring, but we do have to trust that people are taking this task seriously. In the future when we have an electronic system we'll have a better handle on that.

MR. PATTINSON: Thank you.

MR. BEALES: John Sabo.

MR. SABO: Actually it's kind of a follow-up to Neville's question to Kathy and it relates to records that - data or records that may be documenting the use of data. So maybe it could be audit logs or information associated with disclosures as required by the Privacy Act. But audit logs come to mind. I know in the information-sharing environment for business issues you have protected, critical and structured information and a lot of concern about who gets access to it. And in the Privacy Act arena clearly unauthorized access or disclosures or - and associated data with applications might fall under that. How do you address records management of these auxiliary data records? They may not in and of themselves be containing privacy or protected information, but they're mandatory for ensuring that data has not been improperly accessed or altered. Do you deal with that in your records retention policies at all?

MS. SCHULTZ: Yes, we do. For systems that have audit logs we do have a retention for that. I believe that is in the general records schedule published by the National Archives. Generally those issues are handled by the chief information officer's staff. It's not directly records management issue. I'm aware of it, but the practice of audit logs and access by unauthorized people is handled through security and IT. So if they came across a breach, it wouldn't involve me, but they would certainly have processes in place to detect that and determine who was the person that was unauthorized.

MR. BEALES: Do we have other questions? If not I want to thank you both very much for being with us today. We appreciate your appearing in front of us. I believe that brings us to the subcommittee reports on our agenda. The Data Integrity and Information Protection Subcommittee, Reed and Mary I think you are the whole of the subcommittee that's here. I'm not sure there is anything to report, but if there is this is your opportunity. No?

MS. DEROSA: No.

MR. BEALES: No. Okay. Thank you. The Privacy Architecture Subcommittee. Jim Harper.

MR. HARPER: Just briefly I'll recap the projects we have in process, much of which you've heard about before, but we are making progress on these. One is the collaboration with the ISPAB group on privacy architecture, on new thinking about the new problems that we encounter with the advance of information technology and information practices. John Sabo has been a dogged worker on that. We're going to get together with Lesley Reis this afternoon and talk about it more, talk about this collaboration and work on it. There's some good ideas floating around. But in the next few months, by the next meeting or the meeting after that I think we'll have some major work to report on that.

Yesterday I think we had a very profitable meeting on a second, probably the thing that we're most likely to see action on about driving privacy into the grant- making process at DHS. We brought in one of the people from the grants sub-organization at DHS who's very receptive to the idea of bringing the Privacy Office into the fold as far as how they condition grants and what they look for in grants. So we expect that we'll make a recommendation as a committee I hope to get the Privacy Office to weave their thinking into what goes into the grant-making process. So there's I think a lot of room for profitable work there. We want to do the same thing with procurement, but that'll probably take a little bit longer and we have more to learn on the procurement process, if it can be referred to in the singular. I'm not sure. And finally on identification and credentialing, another area of great interest related to REAL ID, but there are many, many more programs and we had a good talk with Kathy Kraninger yesterday. She's receptive to hearing from us and I think she needs to hear some more high-level thinking about the privacy and data integrity issues that surround credentialing programs. So those are the top lines of what we're working on. Thanks.

MR. BEALES: All right, thank you Jim. And the Data Acquisition and Use Subcommittee. I think the report is coming from Kirk.

MR. HERATH: Yes, I'm the vice chair today. We have met, we met yesterday around the REAL ID NPRM. We met a little bit after lunch and our group is going to focus on comments to the REAL ID NPRM. We'll base our comments against fair information practices and our comments will be specific and concrete based upon what is not there and what is there, but probably mostly what is not there. We anticipate having draft comments out to the group by April 2. At least that is going to be our - we're going to attempt that. And then our proposed final comments will be out May 1. So it's a little ambitious, but we don't have a lot of time to get our comments in. So we'll probably have a few calls between now and April 2. Clearly everybody here will have an opportunity to weigh in. That's it.

MR. BEALES: All right, thank you Kirk. I would just note that under our usual procedure which we will follow here the subcommittee will offer up a draft to others who may be interested within the advisory committee and then at some point when that draft goes to the whole advisory committee it will become public and available at that point. And we are anticipating, assuming that everything goes according to plan on this entire somewhat ambitious effort in terms of its timing, we are anticipating having another meeting on or about May 1 to actually discuss that final version of the comment and then approve it in time to actually get it filed by May 2 which is the deadline. So things will be fast and furious on the Data Acquisition and Use Subcommittee and we really appreciate your efforts in trying to make this happen. I know it's a real challenge. There's a

complicated set of substantive issues a really messy set of logistical issues. We really appreciate your effort.

Are there any comments from the committee on the subcommittee reports or questions about the subcommittee reports? If not then we will move on to public comments. We have two people who signed up for public comments and the - you have three minutes to comment. I would note that if you want to talk about REAL ID the advisory committee is very interested in what you have to say and whatever you say will be part of our record, but it will not be a comment on the notice of proposed rulemaking and if you want your comment to be part of the rulemaking record you need to follow the procedures that are set out in the notice of proposed rulemaking. But we don't have to worry about the rulemaking record, so we want to hear what you have to say. Two people signed up for public comments and I would recognize first Steve Howard. And if I could ask you to identify yourself and any affiliation that would be wonderful.

MR. HOWARD: Pleasure to be here. Steve Howard. I'm speaking as an individual, okay. I am working for a company, policy - security that has the opportunity for financial interest in what you're doing, but I spend most of my time working in areas like the Smart Card Alliance on the identity council and physical access councils and things in terms of general policy on this and I've spent a lot of time studying these issues. So I'd like to comment about some of the things we're seeing on REAL ID.

To me one of the things that I learned from the folks at the German Bundespost is that the Bundrucker is doing the design work on the international passport for Germany and their observation to me is one thing is true about ID documents. They are intended to be read. They're there for that purpose. They have to give you secure information and they're intended to be read by the people that we want least to know who we are, probably countries like Iran, Libya, others. So think about that, okay? So in a REAL ID sense we have the same basic objective. The document needs to be readable to be usable. So that's one of the critical things. When we look at identity document fraud, there's a real risk here. Printed features are just not adequate. What we're seeing now and it's showing up in the international passports is that some other means needs to be there to assure the integrity of the data. I believe one of your panel members brought up the issue of the chain of trust. I think it was Neville. Which was the ability to confirm that the document matches the human matches the content. And the digital signature enabling there is absolutely critical. It gives you ease of access, confirmation and it's a better tool to anybody else trying to figure out is this thing real. We actually heard that when we were talking the EEV process that says how do I know that the document that's presented that's being electronically verified is actually the real document. The observation was I don't have to worry about it anymore because I've got EEV. Our challenge is binding the

human to the credential to the verification action. And so we have to make sure that we're capable of doing that.

One observation I want to make and that has to do with the identity numbers that are placed on these things. When we look at the driver's license and REAL ID, one of the things that I've seen in states is that the driver's license tends to never change. It is bound to the human and it is part of the record of the human associated with the relationship to that state. I'd like to recommend that we consider a change to that stance that says the driver's license number needs to change every time I get a new one. That would be very consistent with international passport behavior where the ID is not my Social Security number on my passport, it is a new credential number every time I get the document. So every time I renew my document I get a new one. Now what's the value of this? It allows us to mitigate that the state driver's license becomes a replacement for my Social Security number and it becomes an electronic record identifier that is useful everywhere. I think that's a critical observation. We also need to use a technology that enables the policy in the application context of why am I asking for the data. So the classic example that I've heard recently is an individual who uses their driver's license at a local bar to prove that they are age-appropriate, but it happens to be a young woman and what we're getting is her home address and we're releasing information inappropriately. Whatever technology we use has got to understand the security and integrity of the data on the card and the reason that that card was shown. So when we look at REAL ID we should try and address that. Printed surface features don't allow us to do that and that's going to be a significant challenge.

I'd ask you to consider looking at Gramm-Leach-Bliley and Sarb-Ox and the rules they place on encrypted behavior for financial records because the financial records end up being the source of a lot of the financial fraud which we call identity theft. But when we look at the results and the behaviors of policy that should be applied to the DMVs and how they operate, when we are looking at federated ID I would strongly recommend that this body take a look at the standards that are available for best practices in financial systems and in existing law and regulation around encryption and management of communications to assure that this data is protected at all times.

And I would also ask that we start really looking at existing standards that are already there. To me I'm amazed at the number of times we reinvent what it means to be an ID. I don't get it. There's international driver's license standard available, there's the passport standard available, there's the FIPS Tool 1 standard available. You look at these and the mission objectives very frequently come to the same thing. A credential represents the relationship between the issuer and the bearer, and it binds credential number and appropriate information. So we need to look at what we can do there to mitigate the risks and with that I conclude my comments. Thank you.

MR. BEALES: If I could just ask you briefly, you mentioned the passport numbers change in the international passport context. Does that happen in - I mean the number of the credential changes when it's renewed. Does that happen only in countries that have another national identification system or national identification card of some sort?

MR. HOWARD: No, because my U.S. passport every time I get one, I get a new credential number and I've had three.

MR. BEALES: Okay, thank you.

MR. HOWARD: I think that's an excellent observation.

MR. BEALES: Our last commenter is Tim Corcoran.

MR. CORCORAN: Again, I'm Tim Corcoran. I'm a self-employed consultant security transportation expert in large- scale biometric systems. My background goes back to employment with Global Consultants and International Systems Integrators, program manager for such things as the early INS IDENT program, fingerprints systems, INSPASS, one of the first frequent traveler programs, Mexican voter registration card where we more or less enrolled 48million Mexican voters, welfare systems for Michigan and Illinois and driver's license programs in California in addition to validation and verification of IATHA systems in there. All the issues you've talked about this morning concerning privacy and security, that tradeoff is fine. What I'd like to mention first and this is based on the assumption of what I've heard the board members talk about and some of the other speakers who were here is concerning a business model with respect to governance. The issue is we all understand the regulatory rulemaking process. I'd ask if there is interest on the part of the states in either overturning or objecting to portions of the REAL ID Act due to its timelines, constraints, complexity, lack of specificity with respect to standards. There are existing models out there that have been used successfully for many years. Financial services model, Treasury and Federal Reserve have used for years. The government has incorporated by reference or adopted those rules for security, for privacy, for dispute resolution, thousands of them over the last 30 years. I'd suggest those who are interested might want to take a look at the Electronic Payments Association site and the guidelines shows a very compelling rule, a new governance rule as opposed to just advisory. It in fact puts the commercial sector, in this case the state, in a lead role where the government has an oversight. It has proven to be effective and assertions within the financial community on the government side said we could not have introduced security without the commercial sector or other participants taking a lead as opposed to Treasury and the Federal Reserve. It's out there. It's useful.

Another believe it or not anecdotal, not anecdotal is the National Cattlemen's Beef Associations and their position on the national ID. That's security, it's an infrastructure issue. I suggest you go look at that site as well and the history of the commercial

cattlemen protecting the investment and access to what the government can have, but will respond to all those things with respect to security and the supply chain. Excellent governance models, infrastructure is there.

Two other items. Risk management. We've talked about it, it's been related to these things in the various discussions, but I do not see a specifically hit you in your face what's the risk management approach that was going to be used with respect to REAL ID. I mean it's alluded to, it's referenced to, but that is a requirement for DHS and if this panel is going to make some advice to them, I will do it as well, but with your credentials I think you have a better opportunity to address risk management.

The other one, the identification model that you've seen and you've heard a number of people indicate okay, they are who they say they are. That's what you want to prove. Pointedly, that is the wrong model. Any data modeler in the world will tell you, you know if you're asking Tim Corcoran if I'm Tim Corcoran, I'm giving you a Tim Corcoran document. Might not be forged well, might not be done, but this is not a pedantic point or trivial. It's if you're going into systems design in terms of solutions, the issue is am identifying you based on the relationship of all the objects, people, places, things and events. So in that context that is how identification is done. Much of what is being done with REAL ID again is skewed to the credential. That's fine, but other members on here have talked to it and I think there's an issue within the federal government and the commercial sector that the model they're currently using goes more towards deterrence and cost-to-defeat as opposed to true identification and privacy protection.

Last one and I'm done. Users and participants in here. It's an advisory panel. We addressed the issues of how is this stuff going to be used and I would suggest if there is some means of doing it rather than assert it mode that we start talking about the financial institutions, the banks, the retailers, the medical community, the people who we have generally talked about who are going to use the - possibly use the REAL ID and its mechanisms. And with that, thank you very much for your attention and did I do that in less than three minutes?

MR. BEALES: Close enough.

MR. CORCORAN: Okay.

MR. BEALES: Thank you very much

MR. CORCORAN: Thank you.

MR. BEALES: With that if there are no other questions or comments from the committee as a whole we will adjourn again to our subcommittees to figure out what we're going to do next. Thank you all for coming today and we appreciate your being here.